Title (en)

EFFICIENT CONCURRENT SCALAR PRODUCT CALCULATION

Title (de)

EFFIZIENTE GLEICHZEITIGE SKALARE PRODUKTBERECHNUNG

Title (fr)

CALCUL DE PRODUIT SCALAIRE SIMULTANÉ EFFICACE

Publication

EP 3804214 A4 20210414 (EN)

Application

EP 19806996 A 20190524

Priority

- US 201862676219 P 20180524
- US 2019033933 W 20190524

Abstract (en)

[origin: WO2019226999A1] A method and system for performing a calculation of a privacy preserving scalar product are provided. A first party and a second party (e.g., a first computer and a second computer) possessing a first vector and a second vector respectively, can concurrently determine the scalar product of the two vectors, without revealing either vector to the other party. Each vector can be masked and then encrypted using a public key of an asymmetric key pair. Using homomorphic encryption operations, the scalar product of the vectors can be determined while the vectors are still encrypted. Each party can compare the scalar product, or a value derived from the scalar product against a predetermined threshold. As an example, two parties can perform the scalar product to compare two biometric templates expressed as vectors without revealing the biometric templates to one another, preserving the privacy of persons corresponding to those biometrics.

IPC 8 full level

H04L 9/08 (2006.01)

CPC (source: EP KR)

H04L 9/008 (2013.01 - EP KR); **H04L 9/085** (2013.01 - KR); **H04L 9/14** (2013.01 - KR); **H04L 9/30** (2013.01 - KR); H04L 9/14 (2013.01 - EP); H04L 9/3231 (2013.01 - EP); H04L 9/3234 (2013.01 - EP); H04L 2209/46 (2013.01 - EP)

Citation (search report)

- [I] FEN XU ET AL: "Research on Secure Scalar Product Protocol and Its' Application", WIRELESS COMMUNICATIONS NETWORKING AND MOBILE COMPUTING (WICOM), 2010 6TH INTERNATIONAL CONFERENCE ON, IEEE, PISCATAWAY, NJ, USA, 23 September 2010 (2010-09-23), pages 1 - 4, XP031775322, ISBN: 978-1-4244-3708-5
- [I] WENLIANG DU ET AL: "Privacy-preserving cooperative statistical analysis", PROCEEDINGS / 17TH ANNUAL COMPUTER SECURITY APPLICATIONS CONFERENCE [ACSAC] : 10 - 14 DECEMBER 2001, NEW ORLEANS, LOUISIANA, IEEE, PISCATAWAY, NJ, USA, 10 December 2001 (2001-12-10), pages 102 - 110, XP010584893, ISBN: 978-0-7695-1405-5
- [ID] ARTAK AMIRBEKYAN ET AL: "A new efficient privacy-preserving scalar product protocol", ADVANCES IN ONTOLOGIES, AUSTRALIAN COMPUTER SOCIETY, INC, P.O. BOX 319 DARLINGHURST, NSW 2010 AUSTRALIA, 3 December 2007 (2007-12-03), pages 209 - 214, XP058289053, ISSN: 1445-1336, ISBN: 978-1-920682-36-1
- See also references of WO 2019226999A1

Designated contracting state (EPC)

AL AT BE BG CH CY CZ DE DK EE ES FI FR GB GR HR HU IE IS IT LI LT LU LV MC MK MT NL NO PL PT RO RS SE SI SK SM TR

Designated extension state (EPC)

BA ME

DOCDB simple family (publication)

WO 2019226999 A1 20191128; AU 2019274602 A1 20201126; AU 2019274602 B2 20240502; BR 112020023826 A2 20210413; CN 112166577 A 20210101; CN 112166577 B 20240607; EP 3804214 A1 20210414; EP 3804214 A4 20210414; JP 2021525386 A 20210924; JP 7280285 B2 20230523; KR 20210000722 A 20210105; SG 11202011250X A 20201230

DOCDB simple family (application)

US 2019033933 W 20190524; AU 2019274602 A 20190524; BR 112020023826 A 20190524; CN 201980035074 A 20190524; EP 19806996 A 20190524; JP 2020565425 A 20190524; KR 20207036325 A 20190524; SG 11202011250X A 20190524